What is Cloudflare One?

10/12/2020

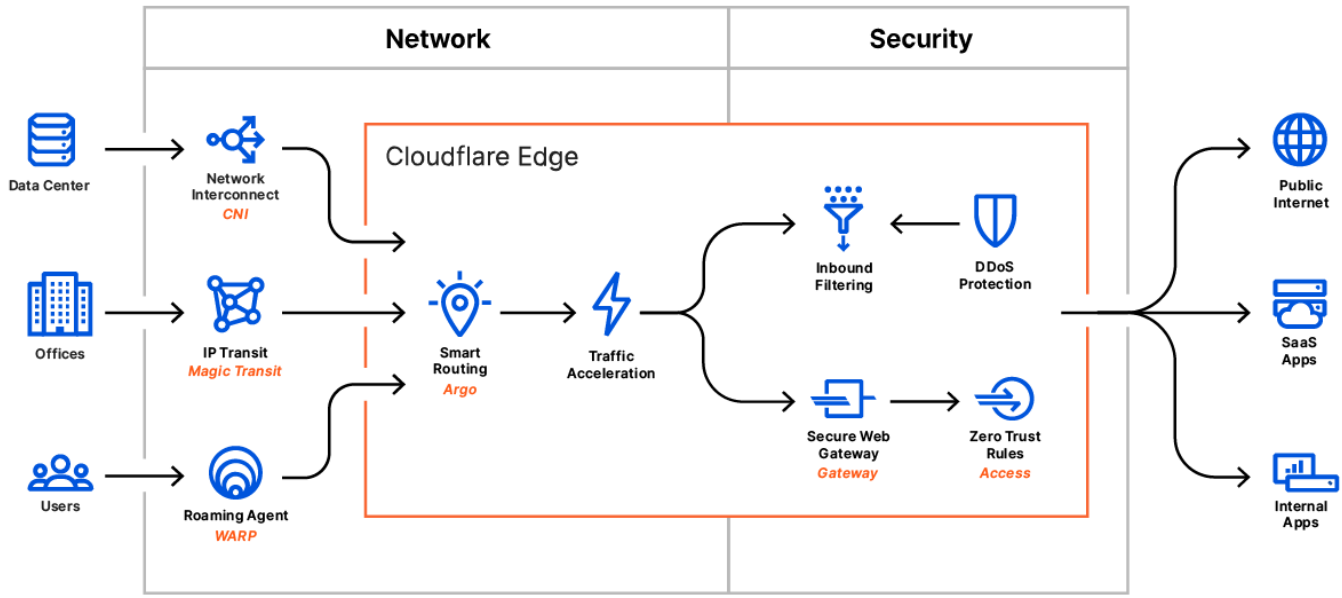
 Rustam Lalkaka  Sam Rhea

Running a secure enterprise network is really difficult. Employees spread all over the world work from home. Applications are run from data centers, hosted in public cloud, and delivered as services. Persistent and motivated attackers exploit any vulnerability.

Enterprises used to build networks that resembled a castle-and-moat. The walls and moat kept attackers out and data in. Team members entered over a drawbridge and tended to stay inside the walls. Trust folks on the inside of the castle to do the right thing, and deploy whatever you need in the relative tranquility of your secure network perimeter.

The Internet, SaaS, and “the cloud” threw a wrench in that plan. Today, more of the workloads in a modern enterprise run *outside* the castle than *inside*. So why are enterprises still spending money building more complicated and more ineffective moats?

Today, we’re excited to share ***Cloudflare One***™, our vision to tackle the intractable job of corporate security and networking.



Cloudflare One combines networking products that enable employees to do their best work, no matter where they are, with consistent security controls deployed globally.

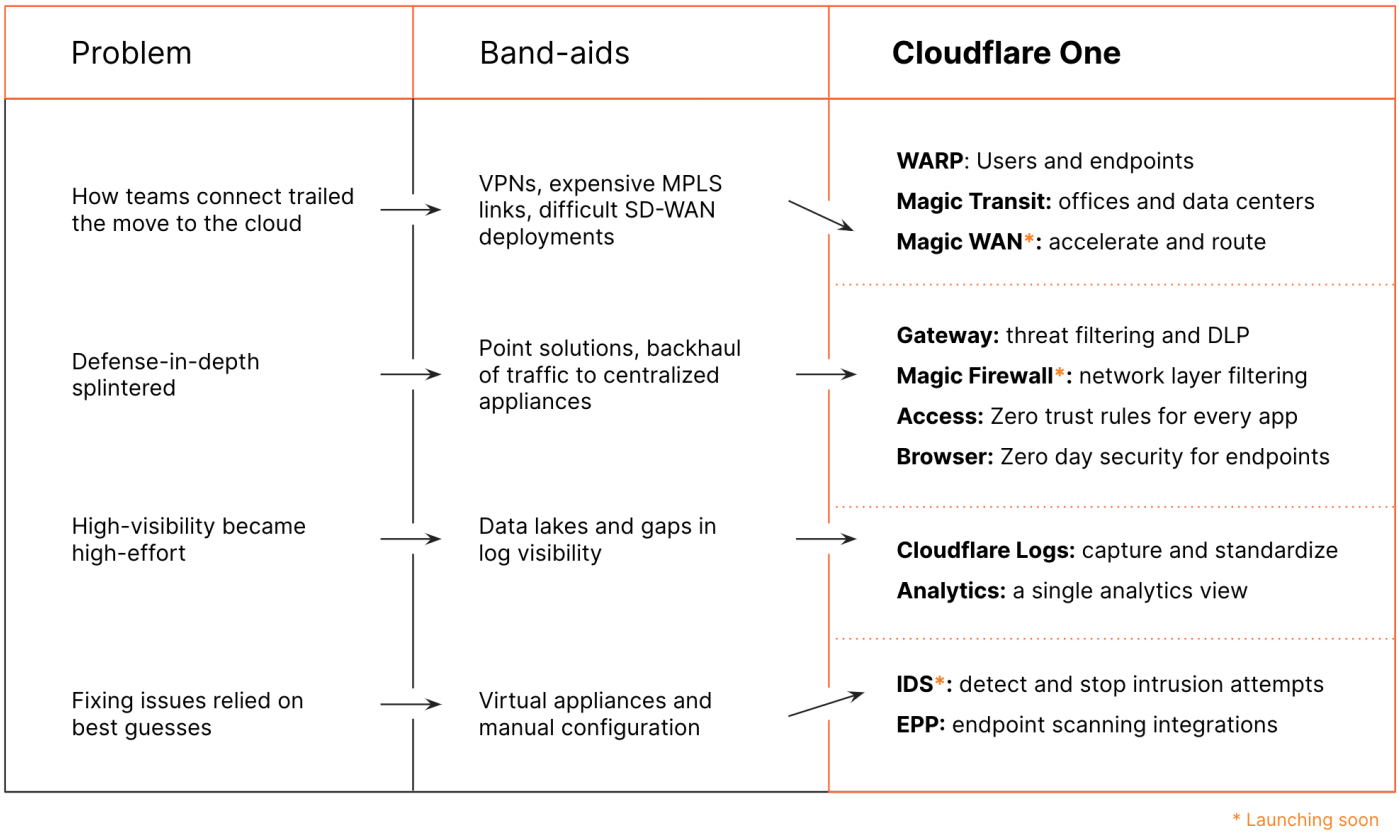
Starting today, you can begin replacing traffic backhauls to security appliances with Cloudflare WARP and Gateway to filter outbound Internet traffic. For your office networks, we plan to bring next-generation firewall capabilities to Magic Transit with Magic Firewall to let you get rid of your top-of-shelf firewall appliances.

With multiple on-ramps to the Internet through Cloudflare, and the elimination of backhauled traffic, we plan to make it simple and cost-effective to manage that routing compared to MPLS and SD-WAN models. Cloudflare Magic WAN will provide a control plane for how your traffic routes through our network.

You can use Cloudflare One today to replace the other function of your VPN: putting users on a private network for access control. Cloudflare Access delivers Zero Trust controls that can replace private network security models. Later this week, we'll announce how you can extend Access to any application -

including SaaS applications. We'll also preview our browser isolation technology to keep the endpoints that connect to those applications safe from malware.

Finally, the products in Cloudflare One focus on giving your team the logs and tools to both understand and then remediate issues. As part of our Gateway filtering launch this week we're including logs that provide visibility into the traffic leaving your organization. We'll be sharing how those logs get smarter later this week with a new Intrusion Detection System that detects and stops intrusion attempts.



Many of those components are available today, some new features are arriving this week, and other pieces will be launching soon. All together, we're excited to share this vision and for the future of the corporate network.

Problems in enterprise networking and security

The demands placed on a corporate network have changed dramatically. IT has gone from a back-office function to mission critical. In parallel with networks becoming more integral, users spread out from offices to work from home. Applications left the datacenter and are now being run out of multiple clouds or are being delivered by vendors directly over the Internet.

Direct network paths became hairpin turns

Employees sitting inside of an office could connect over a private network to applications running in a datacenter nearby. When team members left the office, they could use a VPN to sneak back onto the network from outside the walls. Branch offices hopped on that same network over expensive MPLS links.

When applications left the data center and users left their offices, organizations responded by trying to force that scattered world into the same castle-and-moat model. Companies purchased more VPN licenses and replaced MPLS links with difficult SD-WAN deployments. Networks became more complex in an attempt to mimic an older model of networking when in reality the Internet had become the new corporate network.

Defense-in-depth splintered

Attackers looking to compromise corporate networks have a multitude of tools at their disposal, and may execute surgical malware strikes, throw a volumetric kitchen sink at your network, or any number of things in between. Traditionally, defense against each class of attack was provided by a separate, specialized piece of hardware running in a datacenter.

Security controls used to be relatively easy when every user and every application sat in the same place. When employees left offices and workloads left data centers, the same security controls struggled to follow. Companies deployed a patchwork of point solutions, attempting to rebuild their topside firewall appliances across hybrid and dynamic environments.

High-visibility required high-effort

The move to a patchwork model sacrificed more than just defense-in-depth — companies lost visibility into what was happening in their networks and applications. We hear from customers that this capture and standardization of logs has become one of their biggest hurdles. They purchased expensive data ingestion, analysis, storage, and analytics tools.

Enterprises now rely on multiple point solutions that one of the biggest hurdles is the capture and standardization of logs. Increasing regulatory and compliance pressures place more emphasis on data retention and analysis. Splintered security solutions become a data management nightmare.

Fixing issues relied on best guesses

Without visibility into this new networking model, security teams had to guess at what could go wrong. Organizations who wanted to adopt an “assume breach” model struggled to determine what kind of breach could even occur, so they threw every possible solution at the problem.

We talk to enterprises who purchase new scanning and filtering services, delivered in virtual appliances, for problems they are unsure they have. These teams attempt to remediate every possible event manually, because they lack visibility, rather than targeting specific events and adapting the security model.

How does Cloudflare One fit?

Over the last several years, we’ve been assembling the components of Cloudflare One. We launched individual products to target some of these problems one-at-a-time. We’re excited to share our vision for how they all fit together in Cloudflare One.

Flexible data planes

Cloudflare launched as a reverse proxy. Customers put their Internet-facing properties on our network and their audience connected to those specific destinations through our network. Cloudflare One represents years of launches that allow our network to process any type of traffic flowing in either the "reverse" or "forward" direction.

In 2019, we launched **Cloudflare WARP** — a mobile application that kept Internet-bound traffic private with an encrypted connection to our network while also making it faster and more reliable. We're now packaging that same technology into an enterprise version launching this week to connect roaming employees to Cloudflare Gateway.

Your data centers and offices should have the same advantage. We launched **Magic Transit** last year to secure your networks from IP-layer attacks. Our initial focus with Magic Transit has been delivering best-in-class DDoS mitigation to on-prem networks. DDoS attacks are a persistent thorn in network operators' sides, and Magic Transit effectively defuses their sting without forcing performance compromises. That rock-solid DDoS mitigation is the perfect platform on which to build higher level security functions that apply to the same traffic already flowing across our network.

Earlier this year, we expanded that model when we launched **Cloudflare Network Interconnect** (CNI) to allow our customers to interconnect branch offices and data centers directly with Cloudflare. As part of Cloudflare One, we'll apply outbound filtering to that same connection.

Cloudflare One should not just help your team move to the Internet as a corporate network, it should be faster than the Internet. Our network is carrier-agnostic, exceptionally well-connected and peered, and delivers the same set of services globally. In each of these on-ramps, we're adding smarter routing based on our Argo Smart Routing technology, which has been shown to reduce

latency by 30% or more in the real-world. Security + Performance, because they're better together.

A single, unified control plane

When users connect to the Internet from branch offices and devices, they skip the firewall appliances that used to live in headquarters altogether. To keep pace, enterprises need a way to secure traffic that no longer lives entirely within their own network. Cloudflare One applies standard security controls to all traffic - regardless of how that connection starts or where in the network stack it lives.

Cloudflare Access starts by introducing identity into Cloudflare's network. Teams apply filters based on identity and context to both inbound and outbound connections. Every login, request, and response proxies through Cloudflare's network regardless of the location of the server or user. The scale of our network and its distribution can filter and log enterprise traffic without compromising performance.

Cloudflare Gateway keeps connections to the rest of the Internet safe. Gateway inspects traffic leaving devices and networks for threats and data loss events that hide inside of connections at the application layer. Launching soon, Gateway will bring that same level of control lower in the stack to the transport layer.

You should have the same level of control over how your networks send traffic. We're excited to announce **Magic Firewall**, a next-generation firewall for all traffic leaving your offices and data centers. With Gateway and Magic Firewall, you can build a rule once and run it everywhere, or tailor rules to specific use cases in a single control plane.

We know some attacks can't be filtered because they launch before filters can be built to stop them. **Cloudflare Browser**, our isolated browser technology gives your team a bulletproof pane of glass from threats that can evade known

filters. Later this week, we'll invite customers to sign up to join the beta to browse the Internet on Cloudflare's edge without the risk of code leaping out of the browser to infect an endpoint.

Finally, the PKI infrastructure that secures your network should be modern and simpler to manage. We heard from customers who described certificate management as one of the core problems of moving to a better model of security. Cloudflare works with, not against, modern encryption standards like TLS 1.3. Cloudflare made it easy to add encryption to your sites on the Internet with one click. We're going to bring that ease-of-management to the network functions you run on Cloudflare One.

One place to get your logs, one location for all of your security analysis

Cloudflare's network serves 18 million HTTP requests per second on average. We've built logging pipelines that make it possible for some of the largest Internet properties in the world to capture and analyze their logs at scale. Cloudflare One builds on that same capability.

Cloudflare Access and Gateway capture every request, inbound or outbound, without any server-side code changes or advanced client-side configuration. Your team can export those logs to the SIEM provider of your choice with our **Cloudflare Logpush** service - the same pipeline that exports HTTP request events at scale for public sites. Magic Transit expands that logging capability to entire networks and offices to ensure you never lose visibility from any location.

We're going beyond just logging events. Available today for your websites, Cloudflare Web Analytics converts logs into insights. We plan to keep expanding that visibility into how your network operates, as well. Just as Cloudflare has replaced the "band-aid boxes" that performed disparate network functions and unified them into a cohesive, adaptable edge, we intend to do the

same for the fragmented, hard to use, and expensive security analytics ecosystem. More to come on this soon.

Smarter, faster remediation

Data and analytics should surface events that a team can remediate. Log systems that lead to one-click fixes can be powerful tools, but we want to make that remediation automatic.

Launching into a closed preview later this week, Cloudflare Intrusion Detection System (IDS) will proactively scan your network for anomalous events and recommend actions or, better yet, take actions for you to remediate problems. We plan to bring that same proactive scanning and remediation approach to Cloudflare Access and Cloudflare Gateway.

Run your network on our globally scaled network

Over 25 million Internet properties rely on Cloudflare's network to reach their audiences. More than 10% of all websites connect through our reverse proxy, including 16% of the Fortune 1000. Cloudflare accelerates traffic for huge chunks of the Internet by delivering services from datacenters around the world.

We deliver Cloudflare One from those same data centers. And critically, every datacenter we operate delivers the same set of services, whether that is Cloudflare Access, WARP, Magic Transit, or our WAF. As an example, when your employees connect through Cloudflare WARP to one of our data centers, there is a real chance they never have to leave our network or that data center to reach the site or data they need. As a result, their entire Internet experience becomes extraordinarily fast, no matter where they are in the world.

We expect that performance bonus to become even more meaningful as browsing moves to Cloudflare's edge with Cloudflare Browser. The isolated

browsers running in Cloudflare's data centers can request content that sits just centimeters away. Even further, as more web properties rely on Cloudflare Workers to power their applications, entire workflows can stay inside of a data center within 100 ms of your employees.

What's next?

While many of these features are available today, we're going to be launching several new features over the next several days as part of Cloudflare's Zero Trust week. Stay tuned for announcements each day this week that add new pieces to the Cloudflare One featureset.

	Available Today	**Zero Trust Week**	Coming soon
Connect	Argo Smart Routing Cloudflare Network	WARP + Teams Client Magic Transit APIs	Magic WAN
Defense in depth	Access for self-hosted Apps Magic Transit IP protection	Gateway + Teams Client Access for SaaS Cloudflare Browser (beta)	Magic Firewall
Visibility	Cloudflare Logpush	Gateway Logging	Improved network analytics
Remediation	Endpoint security integrations	Magic Firewall APIs	Intrusion Detection

Discuss on Hacker News

Discuss on Reddit

Cloudflare One Product News Zero Trust Week Zero Trust SASE

Follow on Twitter

Rustam Lalkaka | @lalkaka
Sam Rhea | @LakeAustinBlvd
Cloudflare | Cloudflare

RELATED POSTS

September 28, 2018 8:40PM

Birthday Week Wrap-Up: Every day is launch day at Cloudflare

Our customers are accustomed to us launching new services, features, and functionality at a feverish pace, but recently, we've been especially active. This week we celebrated our 8th Birthday Week by announcing new offerings that benefit our customers and the global Internet community....

By Jake Anderson

Birthday Week, Product News, Registrar, Cloudflare Workers, Cloudflare Workers KV

January 07, 2022 3:57PM

Cloudflare Innovation Weeks 2021

As we start planning our 2022 Innovation Weeks, we are reflecting back on the highlights from each of these weeks...

By Reagan Russell, John Graham-Cumming, Val Vesa

Birthday Week, CIO Week, Developer Week, Full Stack Week, Impact Week

December 09, 2021 1:59PM

How to customize your layer 3/4 DDoS protection settings

Cloudflare Enterprise customers using the Magic Transit and Spectrum services can now tune and tweak their L3/4 DDoS protection settings directly from the Cloudflare dashboard or via the

Cloudflare API....

By Omer Yoachimik

CIO Week, DDoS, L3/4, Managed Rules, flowtrackd

July 30, 2021 3:00PM

The Cloudflare Startup Enterprise Plan: helping new startups bootstrap

To help early stage startups get going, Cloudflare is giving away one year of the Startup Enterprise plan to all early stage startups in participating accelerator programs....

By Jade Q. Wang

Impact Week, Product News, Startup Enterprise Plan, Cloudflare Workers, Cloudflare Stream